IN THE CLAIMS

1. A method for securely transmitting a data message, comprising the steps of:

obtaining a first encrypting key;

generating a second encrypting key as a function of the first encrypting key and as a function of an identified parameter;

encrypting the data message using the second encrypting key to generate an encrypted data message; and

transmitting the encrypted data message.

2. The method of claim 1, wherein the encrypting step corresponds to a public key encryption scheme.

3. The method of claim 2, wherein the encryption scheme is an RSA scheme.

4. The method of claim 1, wherein the encrypting step corresponds to a private key encryption scheme.

5. The method of claim 4, wherein the encryption scheme is a DES scheme.

6. The method of claim 1, wherein the identified parameter is a time or time-dependent value.

7. The method of claim 1, wherein the identified parameter is a randomly generated number.

8. The method of claim 1, further comprising:

receiving the encrypted data message;

obtaining a first decryption key;

generating a second decrypting key as a function of the first decrypting key and as a function of the identified parameter;

decrypting the encrypted data message using the second decrypting key to recover the data message.

9. A method for securely receiving a data message, comprising the steps of:

obtaining a first decrypting key;

generating a second decrypting key as a function of the first decrypting key and as a function of an identified parameter;

decrypting the data message using the second decrypting key to generate the data message.

10. The method of claim 9, wherein the decrypting step corresponds to a public key encryption scheme.

11. The method of claim 10, wherein the encryption scheme is an RSA scheme.

12. The method of claim 9, wherein the decrypting step corresponds to a private key encryption scheme.

13. The method of claim 12, wherein the encryption scheme is a DES scheme.

14. The method of claim 9, wherein the identified parameter is a time or time-dependent value.

15. The method of claim 9, wherein the identified parameter is a randomly generated number.

16. The method of claim 9, wherein the encrypted data message is generated by a method comprising the steps of:

obtaining a first encrypting key;

generating a second encrypting key as a function of the first encrypting key and as a function of an identified parameter;

encrypting the data message using the second encrypting key to generate an encrypted data message; and

transmitting the encrypted data message.

17. A communication system for securely transmitting a data message, comprising:

a memory;

a processor configured to execute the steps comprising:

obtaining a first encrypting key;

generating a second encrypting key as a function of the first encrypting key and as a function of an identified parameter;

encrypting the data message using the second encrypting key to generate an encrypted data message; and

a transmitter for transmitting the encrypted data message.

18. The communication system of claim 17, wherein the encrypting step corresponds to a public key encryption scheme.

19. The communication system of claim 18, wherein the encryption scheme is an RSA scheme.

20. The communication system of claim 17, wherein the encrypting step corresponds to a private key encryption scheme.

21. The communication system of claim 20, wherein the encryption scheme is a DES scheme.

22. The communication system of claim 17, wherein the identified parameter is a time or time-dependent value.

23. The communication system of claim 17, wherein the identified parameter is a randomly generated number.

24. The communication system of claim 17, further comprising a receiver configured to receive the encrypted data message and wherein a second processor is configured to execute the steps comprising:

obtaining a first decryption key;

generating a second decrypting key as a function of the first decrypting key and as a function of the identified parameter;

decrypting the encrypted data message using the second decrypting key to recover the data message.

25. A communication system for securely receiving a data message, comprising:

a memory;

a receiver configured to receive an encrypted data message; and

a processor configured to execute the steps comprising:

obtaining a first decrypting key;

generating a second decrypting key as a function of the first decrypting key and as a function of an identified parameter; and

decrypting the data message using the second decrypting key to generate the data message.

26. The communication system of claim 25, wherein the decrypting step corresponds to a public key encryption scheme.

27. The communication system of claim 26, wherein the encryption scheme is an RSA scheme.

28. The communication system of claim 25, wherein the decrypting step corresponds to a private key encryption scheme.

29. The communication system of claim 28, wherein the encryption scheme is a DES scheme.

30. The communication system of claim 25, wherein the identified parameter is a time or time-dependent value.

31. The communication system of claim 25, wherein the identified parameter is a randomly generated number.

32. The communication system of claim 25, further comprising a transmitter configured to transmit the encrypted data message and wherein a second processor is configured to execute the steps comprising:

obtaining a first encrypting key;

generating a second encrypting key as a function of the first encrypting key and as a function of an identified parameter;

encrypting the data message using the second encrypting key to generate an encrypted data message.

33. A method for securely transmitting a data message, comprising the steps of:

obtaining a first array of encrypting keys;

generating a second array of encrypting keys as a function of the first encrypting key and as a function of an identified parameter;

encrypting the data message using the second array of encrypting keys to generate an encrypted data message; and

transmitting the encrypted data message.

34. The method of claim 33, wherein the encrypting step corresponds to a public key encryption scheme.

35. The method of claim 34, wherein the encryption scheme is an RSA scheme.

36. The method of claim 33, wherein the encrypting step corresponds to a private key encryption scheme.

37. The method of claim 36, wherein the encryption scheme is a DES scheme.

38. The method of claim 33, wherein the identified parameter is a time or time-dependent value.

39. The method of claim 33, wherein the identified parameter is a randomly generated number.

40. The method of claim 33, further comprising:

receiving the encrypted data message;

obtaining a first array of decryption keys;

generating a second array of decrypting keys as a function of the first decrypting key and as a function of the identified parameter;

decrypting the encrypted data message using the second array of decrypting keys to recover the data message.